Filling Cyber-Security Jobs in Government Is Vital

A main challenge for public sector agencies is ensuring they have skilled security professionals who understand the importance of deploying digital technologies securely.

While emerging technologies such as Artificial Intelligence, Intelligent Automation and the Internet of Things are helping to unlock value for public sector organizations, they’re also exposing new security threats and cybersecurity talent gaps.

As we enter October and National Cyber Security Awareness month, it’s concerning that many organizations feel that they are as vulnerable as ever. This is partly because, despite increased cybersecurity spending in recent years, the ‘Threat Gap’—the disparity between current investments in technology, people and processes and what’s needed to mitigate evolving cyber threats—continues to widen.

One of the main challenges for public sector agencies is ensuring they have skilled security professionals in place who understand the importance of developing and deploying new digital technologies securely, as well as the need to protect their organizational data and infrastructure from security threats and breaches.

A recent Accenture study into the state of cybersecurity across the public and private sectors found that two-fifths (42 percent) of security professionals believe they have inadequate budget or resources to hire or train the right security talent. Moreover, almost a third (31 percent) see this lack of training or staffing budget as their single biggest inhibitor to cybersecurity readiness.

The cybersecurity skills shortage

Finding, inspiring and hiring the right security professionals is challenging for government agencies. In a separate Accenture research study, more than half (51 percent) of the public sector agencies surveyed said they look to hire talent from the private sector when deploying technologies across their organizations. In fact, the federal government is hosting its first ever cyber recruitment event in November, where it hopes to fill hundreds of tech and cybersecurity roles across multiple agencies.

However, they face competition with a wide range of organizations for an extremely limited pool of skilled candidates. The Center for Strategic and International Studies recently reported that there could be as many as two million unfilled cybersecurity roles globally by 2019.

This means that the public sector must be flexible – and many are looking to adjacent disciplines for talent. For government agencies, the term ‘security’ doesn’t solely apply to cybersecurity; it also applies to functional security providers such as the intelligence community, border agencies and police forces. As such, public service agencies are increasingly looking to recruit talent from these functional security agencies and apply their intelligence skills and expertise to the challenges of cybersecurity across the public sector.

Public-private partnerships are another important part of the solution. By working together with universities, corporations and other organizations to develop a skills-ready workforce, government agencies will be better prepared to confront evolving digital threats and take a more proactive stance on threat prevention.
While functional security services represent a good source of potential talent, recruiting talent is only half the battle: retention of personnel is equally vital.

**Retaining talent and engaging employees**

In today’s “sellers’ market”, skilled cybersecurity professionals will not stay long in roles that are unrewarding or do not meet their expectations. Therefore, as public sector agencies look to leverage talent from private sector and functional security agencies, employee engagement is critical.

Interestingly, the same technologies that are driving the need for cybersecurity skills also allow for greater employee engagement. By mechanizing repetitive and low-level tasks, Artificial Intelligence and Intelligent Automation allow cybersecurity professionals to focus on higher-level activities, which are generally more interesting and rewarding. Our research shows just how powerful the implementation of emerging technologies can be in increasing employee engagement: 80 percent of respondents believe these technologies will improve job satisfaction among current employees.

Moreover, cybersecurity professionals are more likely to want to work for an organization that uses advanced tools and technologies. By deploying the latest technologies within their operations, public service agencies will gain a reputation for being technically advanced and will attract the skilled employees they need to secure their systems and operations.

An engaged employee population not only improves the retention of skilled cybersecurity professionals, it also provides opportunities to reduce the cybersecurity skills gap among broader employee groups through shared learning and skills transfers – further helping to guard against security threats.

Human error accounts for most cybersecurity incidents, so agencies must actively engage, train and educate all employees about how to recognize and prevent threats. Basic security steps such as training staff in how to recognize phishing emails, the importance of regularly changing their passwords, and regularly testing their knowledge of cybersecurity threats are central to an effective cyber strategy.

**Harnessing Citizen Support**

A recent Accenture survey identified a strong desire among citizens to work with government to fight cybercrime and ensure data privacy and security, with more than half of respondents (58 percent) saying they would undertake national service of some kind to support these efforts.

Some forward-thinking government agencies have already begun to leverage citizen support to enhance cybersecurity defenses. They recognize that even if they’re able to attract, train and retain a skilled cybersecurity team that fully understands the growing impact of emerging technologies, they can’t tackle all security threats alone.

US defense agencies have successfully hosted hackathons where members of their workforce and the public attempt to hack into their IT systems to identify vulnerabilities and security holes. During the 2016 “Hack the Pentagon” event, more than 130 vulnerabilities were reported to the US government.

In the UK, the National Cyber-Security Centre (NCSC) recently launched its Vulnerability Co-ordination Pilot to facilitate public reporting, while both the NCSC agency in The Netherlands and the Australian Cyber-Security Centre (ACSC) run similar programs.
Crowdsourcing cybersecurity allows government organizations to leverage a much wider range of expertise than any one entity alone could hope to possess.

The transformation of public services

It’s hard to overstate the impact new and emerging technologies are having on public service agencies. They are enabling the development of innovative, data-fueled, connected and automated services that will deliver new levels of convenience and efficiency. At the same time, they require new skillsets and a different approach to workforce development and retention.

Tomorrow’s successful organizations will offer employees a more flexible, dynamic environment and the chance to work on projects that truly excite them. These collaborative, forward-looking organizations will have agility – and security – at their core.

Government agencies that don’t fit this description need to act fast to make themselves more attractive to top talent. My advice for agencies is to act now to secure the workforce of the future.

This article was previously published on CIOInsight.com